

PATENT ABSTRACTS OF JAPAN

JPA04-331175

(11)Publication number : 04-331175

(43)Date of publication of application : 19.11.1992

(51)Int.Cl.

B41J 29/38
G03G 15/00
G03G 21/00
H04N 1/44
// G06F 15/00

(21)Application number : 03-276870

(71)Applicant : XEROX CORP

(22)Date of filing : 28.09.1991

(72)Inventor : ROURKE JOHN L
WING PETER D
RATCLIFFE II JACK F
VALLIERE PAUL J

(30)Priority

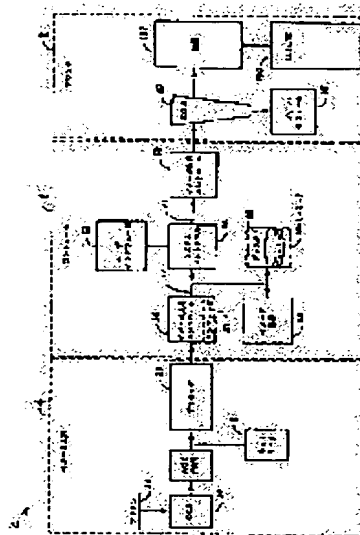
Priority number : 90 591330 Priority date : 28.09.1990 Priority country : US

(54) SECURITY PROTECTING SYSTEM FOR ELECTRONIC PRINTER

(57)Abstract:

PURPOSE: To obtain high security protecting property by limiting an access of other party to a user file, and designating an unremovable security label for the user file for avoiding print or display of the file without security label.

CONSTITUTION: The printing system 2 comprises an image input unit 4 having a remote and on-site image input, a coat roller 7 and a printing unit 8 with a security protecting unit. The protecting unit specifies an individual security profile for a user of different class by managing by a decided security manager. An identification number is further specified, and use of a user's password is allowed. Further, a site manager is specified. A user job programming option management is given to the manger, and a role of the site manager is separated from the user's role.



Best Available Copy

This Page Blank (As per)

JPA04-331175

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平4-331175

(43) 公開日 平成4年(1992)11月19日

(51) Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
B 4 1 J 29/38		Z 8804-2C		
G 0 3 G 15/00	1 0 2	8004-2H		
	21/00	6605-2H		
H 0 4 N 1/44		2109-5C		
// G 0 6 F 15/00	3 3 0 A	7323-5L		

審査請求 有 請求項の数6 (全 24 頁)

(21) 出願番号 特願平3-276870

(22) 出願日 平成3年(1991)9月28日

(31) 優先権主張番号 5 9 1 3 3 0

(32) 優先日 1990年9月28日

(33) 優先権主張国 米国 (U S)

(71) 出願人 590000798

ゼロックス コーポレーション
 XEROX CORPORATION
 アメリカ合衆国 ニューヨーク州 14644
 ロチェスター ゼロックス スクエア
 (番地なし)

(72) 発明者 ジョン・エル・ローク

アメリカ合衆国 ニューヨーク州 14450
 フエアポート ウォーターフオードウェイ 94

(74) 代理人 弁理士 小堀 益

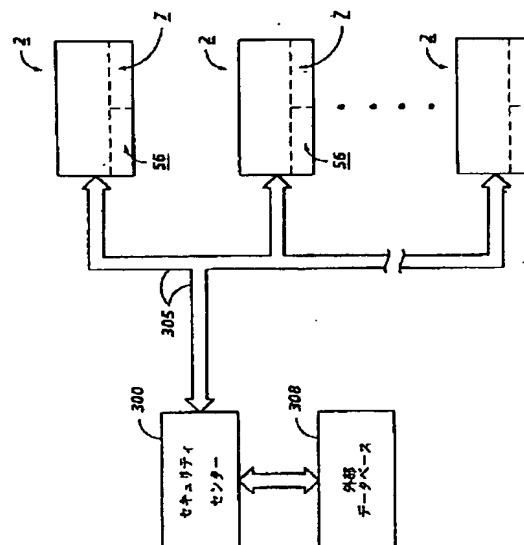
最終頁に続く

(54) 【発明の名称】 電子印刷機の機密保護システム

(57) 【要約】 (修正有)

【目的】 電子プリンタおよび印刷機の機密保護装置の提供。

【構成】 セキュリティ管理者を決定する工程と、セキュリティプロフィールを規定する工程と、セキュリティ管理者の能力を、ユーザに識別番号を指定する工程と、ユーザによるパスワードの使用を可能にする工程と、サイト管理者を規定する工程と、サイト管理者に対してユーザジョブプログラミングオプションの管理を付与する工程と、ユーザの役目からサイト管理者の役目を分離する工程と、ユーザに対し、ユーザファイルを保護し、ユーザファイルに対し他者のアクセスを制限し、セキュリティラベルなしに、ファイルの印刷または表示が回避されるユーザファイルに対し、除去不可能なセキュリティラベルを指定することができるようにすることによって、ユーザファイルセキュリティを規定する工程からなる。



【特許請求の範囲】

【請求項1】 次のステップを含む、電子写真複写印刷機の機密保護方法：

- a) セキュリティ管理者を決定する；
- b) 前記セキュリティ管理者の管理下で異なるクラスのユーザに対し個別のセキュリティレベルを備えたセキュリティプロフィールを規定する；
- c) 前記セキュリティ管理者の能力を、
 - 1) 機密保護が不十分なサイトにおいてユーザに識別番号を指定する；
 - 2) 機密保護が充分なサイトにおいてユーザによるパスワードの使用を可能にする；
 - d) サイト管理者を規定する；
 - e) 前記印刷機のために前記サイト管理者に対してユーザジョブプログラミングオプションの管理を付与する；
 - f) 特定の識別番号およびパスワードを前記サイト管理者に指定し、前記サイト管理者の役目へのユーザのアクセスを阻止することによって、ユーザの役目から前記サイト管理者の役目を分離する；そして
 - g) ユーザに対して

- 1) ユーザパスワードによってユーザファイルを保護し、
- 2) ユーザファイルに対して他者のアクセスを制限し、
- 3) 前記セキュリティレベルなしに前記ファイルの印刷または表示が回避されるユーザファイルに対して、除去不可能なセキュリティレベルを指定することができるようにすることによってユーザファイルセキュリティをユーザに規定する。

【請求項2】 プリントプログラミング特性へのユーザのアクセスを制限することによってユーザファイルセキュリティを規定するステップを含む請求項1に記載の方法。

【請求項3】 ファイルの移動または変更のみを許容するプリントプログラミング特性へのユーザのアクセスを制限することによってユーザファイルセキュリティを規定するステップを含む請求項1に記載の方法。

【請求項4】 複雑なプリントプログラミング特性へのアクセスを制限してプリンタのダウンタイムを回避するステップを含む請求項1に記載の方法。

【請求項5】 予め選択されたプリントプログラミング特性へのユーザのアクセスを制限してプリンタの個人的使用をなくす請求項1に記載の方法。

【請求項6】 次のものの組み合わせ；

- a) ユーザパスワードを含むセキュリティデータを記憶するための内部セキュリティデータを有する電子プリンタと；
- b) 特定のユーザ識別番号を含むユーザプロフィールを記憶するための外部許可データベースと；
- c) プリセット識別番号を、前記ユーザに許容されるに必要とされる個々のユーザまたはグループをなすユーザ

に指定し、個々のパスワードの使用を可能にされた少なくともある数の前記ユーザに対し前記システムのアクセスを許容する少なくとも一つのセキュリティ管理者に資格を付与する手段と；

d) 前記パスワードが前記内部データベースに記憶されており；

e) 前記ユーザに対して、他のユーザの権利への選択的制限を課し、ユーザのジョブファイルを変更することの可能な手段と；

10 f) ユーザが自分の識別番号およびパスワードを入力する必要性を課せられている前記外部許可データベースを前記プリンタに接続し、前記プリンタにアクセスする通信チャネルと；

g) 前記外部許可データベース中の識別番号をユーザによって入力された前記識別番号と照合する手段と；

h) 前記ユーザパスワードを前記内部データベース中のパスワードと照合する手段と； 1) 有効な識別番号およびパスワードを設定し、前記ユーザに対し前記プリンタへのアクセスを可能にする手段。

20 【発明の詳細な説明】

【0001】本発明は電子プリンタおよび印刷機に関し、より詳しくは電子プリンタおよび印刷機の機密保護装置に関する。

【0002】従来の光／レンズ式複写機において、文書の機密保護は概して文書原稿の物理的重要性と複写された複写物に基づいており、一方複写機のアクセスおよび利用は課金の考え方に基づいている。文書の機密保護の場合、ユーザの原稿および複写物の機密保護には次のような事実が付随している。すなわち、複写された複写物自体だけでなく、複写物の作られる原稿も通常所有物中に残っており、所有者の管理または複写物の作成が委託されている所有者の知っているだれかの管理下にある。仮にそれが存在しているとして、複写機へのアクセスされることに対する管理は一般的に複写機を使用する者および複写をする者が作成された複写物に対して正確な請求を受けているかどうか保証されることに基づいていた。これは例えば、過去において複写物の料金が請求できる口座を有している者への複写機の使用が制限されていた。このことが複写料金カウンタまたはメータの開発と導入の先駆けとなった。しかし、概して、複写機環境において、機密保護に対してほとんど、またはまったく注意が払われていなかった。特に、所有者のファイルの機密保護についてはそうであった。

【0003】しかし、複写機の出現により、イメージが電気信号または画素である場合、実際に秘密であったり、個人のものであるユーザの電子ファイル、プログラム等は少なくともシステムに一般的に記憶される。この結果、所有者のファイルにはだれでもこれを読み取ったり、複写したり、改ざんしたりすべくシステムにアクセスすることができ。同様の状況がシステム間の送受用

通信チャネルに伝達されるデータにおいても発生する。システムにアクセスしようとする者はだれでも自分自身のために、伝達されたデータへのアクセスを傍受し、得ることができる。

【0004】従来技術において、過去の機密保護は米国特許第4,713,753号に明示されているようにデータプロセッサのためのセキュリティシステムアーキテクチャに開示されたコンピュータシステムに焦点が合っている。前述のアーキテクチャにおいてセキュリティプロセッサに記憶された予め規定されたセキュリティポリシーはプログラムの変更を阻止するようにフォーマットコントロールを用いている。米国特許第4,525,780号、同第4,498,132号（その記述は同第4,525,780号に依存している）が、情報に対するアクセス権を処理するアドレスシステムを有するデータ処理システムが開示されている。また、米国特許第4,799,258号にはコンピュータへのアクセスを管理し改ざん阻止記憶を保証するデュアルキーシステムが開示されている。

【0005】さらに、コンピュータアプリケーションにおいて、ユーザ識別コード（UIC）技術がファイルアクセスを管理するのに使用されてきている。この技術において、二つの番号、すなわち、グループ番号およびメンバー番号が1人のユーザにつき用意されている。従って、各ユーザはグループの一員となる。他のユーザ番号と共通の必要事項との橋渡した情報を分担する。さらに、各ファイルは、読み取りおよび書き込みアクセスをコントロールする所有者および保持セキュリティのUIC等の関連するある種の属性を備えている。しかし、このUIC等の関連するある種の属性を備えている。しかし、このUICシステムは機密保護はあるが拡張度が制限されたレベルの点で制限がある。

【0006】前述の米国特許第4,498,132号および同第4,525,780号に開示されている第2の先行技術はアクセスリストに基づいており、ファイルの各操作は、アクセスが認められているか、または、拒否されているユーザのファイル所有者によって維持されたリストによって管理される。さらに、このリストは予め規定されたグループおよび対象の可能範囲または制限規定を含んでいる。この技術の欠点は必要とするメモリが大量であり、リストを維持し、調節することを必要とするプロセス所有者ヘッドが多量であるということである。

【0007】これとは逆に、本発明は電子写真複写印刷機の機密保護方法を提供する。この方法は、セキュリティ管理者を決定する工程と；前記セキュリティ管理者の管理下でユーザの異なるクラスのユーザに対し個別のセキュリティレベルを備えたセキュリティプロフィールを規定する工程と；前記セキュリティ管理者の能力を、機密保護が不十分なサイトにおいてユーザに識別番号を指

定する工程と；機密保護が十分なサイトにおいてユーザによるパスワードの使用を可能にする工程と；サイト管理者を規定する工程と；前記印刷機のために前記サイト管理者に対してユーザジョブプログラミングオプションの管理を付与する工程と；特定の識別番号およびパスワードを前記サイト管理者に指定し、前記サイト管理者の役目へのユーザのアクセスを阻止することによって、ユーザの役目から前記サイト管理者の役目を分離する工程と；ユーザに対して、ユーザパスワードによってユーザファイルを保護し、ユーザファイルに対して他者のアクセスを制限し、前記セキュリティラベルなしに前記ファイルの印刷または表示が回避されるユーザファイルに対して、除去不可能なセキュリティラベルを指定することができるようにすることによってユーザファイルセキュリティを規定する工程と；から成ることを特徴とする。

【0008】〔図面において〕図1は本発明の機密保護システムに併用する電子印刷機を示す図である。

【0009】図2は図1に示す印刷機の主要素を示すブロック図である。

【0010】図3は図1に示す印刷機の主たる機械要素を示す平面図である。

【0011】図4は図1に示す印刷機の文書スキャナの特定部分の構造の詳細を示す説明図である。

【0012】図5,6および7は図1に示す印刷機の制御部の主要部を示すブロック図である。

【0013】図8は図1に示す印刷機のための操作システムをプリント配線基板および共通ライン接続と共に示すブロック図である。

【0014】図9は図1に示す印刷機のユーザインタフェース（UI）タッチスクリーン上に表示された典型的なジョブプログラミングチケットおよびジョブスコアカードを示す図である。

【0015】図10はユーザインタフェースタッチスクリーンを示す図であり、タッチスクリーン上に「ユーザ」、「セキュリティプロフィール」および「アクセスリスト」を名前でユーザのリストを表示するように作動された「ユーザ」アイコンと共に有する「セキュリティ」カードファイルが表示される。

【0016】図11はユーザがハイライトすることと、プロセスセレクションを規定するシステム管理者ウィンドウをオープンすることによって選択されることを示す図である。

【0017】図12は選択されたユーザのユーザプロフィールを表示する図である。

【0018】図13は選択されたユーザの「特権」カードファイルを示す図である。

【0019】図14はオープンされた「ユーザ削除？」オプションウィンドウを示す図である。

【0020】図15はオープンされた「新規所有者選定？」オプションウィンドウを示す図である。

【0021】図16はオープンされた「ユーザプロフィールオプション」ウインドウを示し、「新規ユーザテンプレート」選択を表示する図である。

【0022】図17は「新規ユーザテンプレート」次選択を示すユーザインタフェースタッチスクリーンを示す図である。

【0023】図18はサイト用「セキュリティプロフィール」カードファイルを示す図である。

【0024】図19はサイト用「アクティビティログ」を示す図である。

【0025】図20は図19の「アクティビティログ」をオープンされた「オーディットトレイル（鑑査手がかり）オプション」ウインドウと共に示す図である。

【0026】図21は「アクセスリスト」カードファイルを表わすユーザインタフェースタッチスクリーンを示す図である。

【0027】図22はリスト選択を表示すべくオープンされたファイルウインドウと共に図21の「アクセスリスト」カードファイルを示す図である。

【0028】図23はオープンされた「リスト削除？」ウインドウと共に図21の「アクセスリスト」カードファイルを示す図である。

【0029】図24は選択されたアクセスリスト中のメンバーの名前で「メンバー名」ファイルを示す図である。

【0030】図25は選択されたアクセスリストからメンバーを除外する「リストからの削除」選択ウインドウを示す図である。

【0031】図26は選択されたアクセスリストにメンバーの名前を加えるための「メンバー追加」ウインドウを示す図である。

【0032】図27はファイル所有者をしてアクセス権をファイル所有者に設定せしめる「ジョブアクセス制御」カードを示す図である。

【0033】図28は機密保護システムが外部から管理される第2実施例を示す図である。

【0034】図1、図2において、本発明の技術による印刷ジョブを実行する典型的なイメージ印刷システム2を示す。説明の都合上、印刷システム2をイメージ入力部4と、コントローラ部7と、プリンタ部8に分割する。図示例において、イメージ入力部4は印刷システム2をネットワーク、操作および印刷動作せしめる遠隔およびオンサイトイメージ入力を有している。他の装置の組合せも、例えば、オンサイトイメージ入力（すなわち、スキャナ）、コントローラおよびプリンタを備えた印刷システム；遠隔入力、コントローラ、プリンタを備えたネットワーク印刷システム等も考慮することができる。特定の印刷システムを図示し説明するが、本発明は他の印刷システムとの併用も可能である。例えば、プリンタ部8はインクジェット、イオノグラフィック等の別

のタイプのプリンタも代りに用いることもできる。

【0035】図2～図4において、オフサイトイメージ入力につきイメージ入力部4がネットワーク5を有している。このネットワークは処理の目的で印刷システム2へ入力されるべき一つまたはそれ以上の遠隔ソースからのイメージ信号または画素からイメージデータを得る電話線等の適当な通信チャネルを備えている。入ってくるイメージデータのページ記述言語（PDL）が印刷システム2によって用いられたPDLとは異なる場合には、適当な変換手段（図示省略）が設けられる。ストリーミングテープやフロッピーディスク等のイメージデータの遠隔ソースも考えられる。

【0036】オンサイトイメージ入力に対しては、イメージ入力部4はその上に走査されるべき文書22が載置されている透明プラテン20を備えた文書スキャナ6を有している。一つのまたはそれ以上のリニアアレイ24がプラテン20の下方で往復走査移動をするために支持されている。レンズ27およびミラー28、29、30が協同して、プラテン20へのライン上セグメントおよびその上で走査されるべき文書上にアレイを焦点合せする。ネットワーク5またはアレイ24からのイメージ信号または画素の形をなすイメージデータが処理のためにプロセッサ25に入力される。

【0037】プロセッサ25はアレイ24によってアナログイメージ信号出力をデジタルに変換する。プロセッサ25はプログラムされたジョブを印刷システムに実行させるのに必要な形にイメージ信号をさらに処理する。プロセッサ25はフィルタし、しきい値を出し、スクリーニングすること等イメージ信号のエンハンスメントおよび変化の施しもある。

【0038】走査されるべき書類22は再循環文書処理（RDH）モードまたは半自動書類処理（SADH）モードのいずれかで動作可能な自動文書処理装置（ADF）によって走査するためにプラテン20上に載置される。ブックモードおよびコンピュータフォームズフィーダ（CFF）モードを含むマニュアルモードも備えており、後者は文書をコンピュータファンホールドの形で収容する。RDHモード操作のために、文書ハンドラー35がトレイ37を有しており、ここに文書が積み重ねられるか束ねられて収容されている。トレイ37中の文書22は真空供給ベルト40、文書供給ローラ41および文書供給ベルト42によってプラテン20上に進行され、プラテン上で書類がアレイ24によって走査される。走査に続いて、書類はベルト42によってプラテン20から除去され書類供給ローラ44によってトレイ37に戻される。

【0039】SADHモードでの走査のために、文書挿入スロット46が文書トレイ37とプラテン20間の文書供給ベルト42にアクセスできるように設けられており、各文書がプラテン20上に移送されるべくこのスロ

7

ットから手で挿入される。スロット46の前方の供給ローラ49がニップを形成しており、文書を係合して文書供給ベルト42からプラテン20に供給される。走査工程に続いて文書はプラテン20から除かれキャッチトレイ48に放出される。

【0040】CFFモードの走査のために、コンピュータで作られた材料がスロット46から供給され、供給ローラ49によって文書供給ベルト42に送られ、次に折りたたまれた文書の1頁がプラテン20上に送られる。

【0041】図2、図3を参照して、プリンタ部8はレーザプリンタから成り、説明の都合上ラスタ出力スキャナ(ROS)部87、プリントモジュール部95、給紙部107および仕上部120に分割する。ROSはレーザ91を有しており、そのビームは二つのイメージビーム94に分けられる。各ビーム94は音響-光学モジュレータ92によってイメージ信号入力の内容に基づいてモジュレートされ二重イメージビーム94が作られる。ビーム94はプリントモジュール部95の移動している感光体98を横切るようにして回転多角体100の鏡面によって走査されそれぞれの走査により感光体98が二つのイメージで露光され、かつ、イメージ信号入力によって表わされる潜在静電イメージが音響-光学モジュレータ92に作られる。感光体98はイメージビーム94によって露光されるべく用意された帯電部においてコロトロン102によって均一に帯電される。潜在静電イメージは現像機104によって現像され、転写部106において給紙部107によって運ばれた印刷媒体108に転写される。出てくることの予想される印刷媒体108は種々のサイズ、タイプおよび色のシートが含まれる。転写につき、印刷媒体は感光体98上に現像されたイメージと時間調節された状態で主ペーパートレイ110または補助ペーパートレイ112、114から送られる。印刷媒体108に転写された現像イメージはヒューザ116によって永久的に付着または溶着され、得られたプリントはアウトプットトレイ118または仕上装置120に放出される。仕上装置120はプリントをステッチを施すか、ステーブル打ちするステッチャ122およびプリントを本として接着束ねるための熱バインダを含んでいる。

【0042】図1、図2および図5を参照して、説明の都合上、コントローラ部7をイメージ入力制御器50、ユーザインタフェース(UI)52、システムコントローラ54、メインメモリ56、イメージマニプレーション部58およびイメージ出力コントローラ60に分割する。

【0043】イメージ入力部4のプロセッサ25からコントローラ部7に送られるイメージデータ入力はプリント配線基板(PWB)70-3のイメージ入力コントローラ50のイメージコンプレッサ/プロセッサ51によって通過されると、イメージデータは、スライスポイン

8

タを有するN本の走査ライン幅のスライスに分割される。スライスポインタおよびイメージ特定情報(画素による文書の高さと幅、使用された圧縮方法、圧縮されたイメージデータに対するポインタおよびイメージスライスポインタに対するポインタ等)のイメージ特定情報を有するあらゆる関連するイメージ記述子と共に圧縮されたイメージデータがイメージファイルに配置される。異なるプリントジョブを表わすイメージファイルは、ランダムアクセスメモリまたはRAMから成るシステムメモリ61に、データの使用中保護されているイメージメモリ56に転送している間、一時的に記憶される。

【0044】図1に最もよく示すように、ユーザインタフェース(UI)52は対話型タッチスクリーン62、キーボード64およびマウス66から成る。UI52は印刷システム2とオペレータとをインタフェースして、オペレータがプリントジョブや他の命令をプログラムし、印刷システムの操作情報、命令、プログラム情報、診断プログラム等々を得ることができる。タッチスクリーン62上に表示されるファイルおよびアイコン等の項目がタッチスクリーン62上の表示された項目を指またはマウスを用いて動作させ、カーソル67を指示し、選択された項目を指示し、マウスをキーイングする。

【0045】メインメモリ56は機械操作システムソフト、機械操作データおよび目下処理されつつある走査イメージデータを記憶する複数のハードディスク90-1、90-2、90-3を有している。

【0046】メインメモリ56の圧縮されたイメージデータがさらに処理を必要とするか、またはUI52のタッチスクリーン62上に表示が必要か、またはプリンタ部8によって必要とされている場合に、データはメインメモリ56にアクセスされる。プロセッサ25によって実行された以外のさらなる処理が必要な場合、データはPWB70-6のイメージマニプレーション部58に転送され、ここで照合、準備、分析等の付加的な処理工程が実行される。処理に続いて、データがメインメモリ56に戻され、タッチスクリーン62に表示するためにUI52に送られるか、またはイメージ出力コントローラ60に送られる。

【0047】イメージ出力コントローラ60に出力されたイメージデータは圧縮が解除され、PWB70-7、70-8(図5参照)のイメージ発生プロセッサ86によって印刷されるために準備される。これに続いて、データがPWB70-9上のディスパッチプロセッサ88、89によってプリンタ部8に出力される。印刷のためにプリンタ部8に送られるイメージデータは新しいイメージデータの場所をあけるべく通常メモリ56から追出される。

【0048】図5-7を参照して、コントローラ部7が複数のプリント配線基板(PWB)70を含んでおり、このPWB70は互いに接続され、さらに一対のメモリ

バス72、74によってシステムメモリ61に接続されている。メモリコントローラ76はバス72、74でシステムメモリ61に接続されている。PWB70は複数のシステムプロセッサ78を有するシステムプロセッサPWB70-1と；データをUI52に送り、またこれからデータを受けるためのUI連絡コントローラ80を有する低速I/OプロセッサPWB70-2と；データをメインメモリ56のディスク90-1、90-2、90-3それぞれに送り、またこれからデータを受けるためのディスクドライブコントローラ/プロセッサ82を有するPWB70-3、70-4、70-5（イメージデータを圧縮するためのイメージコンプレッサ/プロセッサ51はPWB70-3に在る）と；イメージマニプレション部58のイメージマニプレションプロセッサを備えたイメージマニプレションPWB70-6と；プリンタ部8によって印刷するためイメージデータを処理するためのイメージ発生プロセッサ86を備えたイメージ発生プロセッサPWB70-7、70-8と；プリンタ部8間のデータの送受をコントロールするためのディスパッチプロセッサ88、89を有するディスパッチプロセッサPWB70-9と；ブートコントロールアービトレーションスケジューラPWB70-10と；を含んでいる。

【0049】図8を参照して、システムコントロール信号が複数のプリント配線基板（PWB）を介して分配されている。これらのプリント配線基板にはEDNコアPWB130と、マーキングイメージングコアPWB132と、バーバ処理コアPWB134と、種々の入力/出力（I/O）PWB138を備えたフィニッシュバインダコアPWB136を含んでいる。システムバス140がコアPWB130、132、134、136を互いに接続し、さらにコントローラ部7と接続している。一方ローカルバス142がI/O PWB138を互いに接続し、さらにそれらの関連するコアPWBと接続する働きをしている。

【0050】印刷システムの能力を増大させると、操作システムソフトがメモリ56からEDNコアPWB130に、またこのPWB130からバス140を介して残りのコアPWB132、134、136に装荷される。各コアPWB130、132、136は操作システムソフトのPWB、故障検出等への脱荷を制御するためのブードROM147を有している。ブードROM147は操作システムソフトとの間における制御データの送受、およびローカルバス140を介してのI/O PWB130、132、134、136間での制御データの送受、さらにローカルバス142を介してのI/O PWB138との間の制御データを送受も行なう。付加的ROM、RAMおよびNVMメモリ等は印刷システム2内の種々の位置に設けられている。

【0051】図9を参照して、ジョブはジョブプログラ

ムモード内でプログラムされる。このジョブプログラムにおいて、タッチスクリーン62上にプログラムされるべきジョブのためのジョブチケットおよびジョブスコアカード152が表示される。ジョブチケット150にはプログラムされる種々のジョブ選択項目が表示され、一方ジョブスコアカード152には、ジョブを印刷するためにシステムへの基本命令事項が表示される。

【0052】システムメモリに記憶されたサイトにおいて印刷システム2へのアクセスを制御し、あらゆる感知データを保護するために、本発明の機密保護装置が備えつけられる。実行するにあたり、印刷システム2へのアクセスを進めるためにユーザは 特定のユーザ認証番号（ユーザID）を証明する必要がある。パスワードにオプションがある場合は、ユーザは自分のパスワードを登録する必要がある。明らかなように、機密保護装置がユーザIDを指定し、一方ユーザはそれが認められたときに自分自身のパスワードを作る。

【0053】印刷システム2の営業場所であるサイトで所望のセキュリティレベルを定義する能力を有している。概して、セキュリティレベルは：

【0054】（1）サイト管理者またはセキュリティ管理者のいずれかによって調整された管理機能以外機密保護性はない。これらの管理機能は感知情報およびシステムによって変化する能力を保護するアクセスコントロールを必要とするタイプである。このセキュリティレベルではどのユーザを印刷システムにログオンする必要はなく、各ユーザは印刷システムで利用可能なあらゆる機能に完全にアクセスできる。

【0055】（2）部分的に機密保護されたサイトが、セキュリティ管理者の選択の自由で、あるユーザに対して認証されるべきユーザIDを許容する。これはこれらのユーザに対してある一定の特定のシステム機能にアクセスを与えるものである。

【0056】（3）すべてのユーザがセキュリティ管理者によってユーザIDを承認した完全に機密保護されたサイト。

【0057】（4）パスワードのある完全に機密保護されたサイトがセキュリティ管理者の選択の自由において、あるユーザまたは全ユーザに対してユーザ自身のパスワードを用いてシステム中のユーザ自身のファイルへのアクセス制御を許容する。

【0058】サイト管理者は通常定められている（しかし、一人の管理者がサイトおよびセキュリティ管理者の資格を兼務できる）。サイト管理者は特定ユーザとみなされており、だからして特定ユーザまたは非特定ユーザの特権のいずれに対してもある特権を有している。典型的にはサイト管理者はサイトが持っているプログラムの特徴および機能、システムの不履行設定等を設定し、さらに料金請求、料金計算等の操作機能を分担する。

【0059】セキュリティ管理者はサイトによって求め

られている機密レベルと一致した印刷システム2の機密規則を作成し、実行する責任を負わされた信用されている個人である。この資格において、セキュリティ管理者は印刷システム2のプログラミング特性、管理およびサービスへのアクセスを管理する。プログラミング機能および特性はサイト管理者によってユーザに対して利用可能にするシステムジョブプログラミングの選択の異なるレベルから成る。セキュリティ管理はサイトにおける機密が管理されることによるプロセスに関係し、一方、サービスはサービスまたは修理担当者（ここでは技術修理者（Tech Reps））によるアクセスを管理する機密保護に関係する。

【0060】セキュリティ管理者がその任務の実行を可能とするために、各ユーザのユーザプロフィールを設定し維持する。ユーザプロフィールはセキュリティ管理が各ユーザのセキュリティプロフィールの設定を許容されているものである。ここで各ユーザはセキュリティ管理者によってユーザIDにユーザパスワード、サイトの機密レベルに依存した異なるシステムプログラミング機能等へのアクセス権のような他のセキュリティ可能性を加えて保証された者である。理解できるであろうが、ユーザプロフィールへのアクセスはセキュリティ管理者の有している権利の範囲内である。

【0061】図10～12を参照して、「管理」モードに入る「ユーザプロフィールモジュール」がタッチスクリーン62に表示される、あるカードファイルには各々「ユーザ」、「セキュリティプロフィール」および「アクセスリスト」アイコン201、202、203が表示された「セキュリティ」カードファイル200が含まれている。「ユーザ」アイコン201の作動が表示されるべき「ユーザ名」ファイル205をしてサイトにおける全ユーザの名前をリストせしめる。このファイル205には指定された一人のユーザID、複数のユーザID、およびユーザが「アクティブ」であるか「イナクティブ」であるかを表示する。上下スクローリングアイコン207、208がファイル205をスクローリングし、すべてのユーザの名前の読みを可能にする。

【0062】セキュリティ管理者が特定ユーザプロフィールを検視したい場合、「ユーザ名」ファイル205中の「ユーザ」アイコン210が作動され、「プロフィールを開く」、「アクティブ」、「削除」および「閉じる」選択項目を有する「システム管理」ウインドウ212に表示される。移動しているウインドウ212、すなわち、ウインドウポインタ212'がユーザの名前の向側にある、そのユーザのユーザプロフィールが検視され、作動している「オープニングプロフィール」が選択されたユーザ名をユーザプロフィールに表示する。図12に示すように、ユーザプロフィール215は「ユーザステータス」、「ユーザ名」、「ユーザID」を識別し、ユーザパスワードを有しているか否か、およびユーザの「不履行アカ

ウント(Default Account)」を識別表示する。加うるに、「ジョブアクセス制御」アイコン217および「特権(Privileges)」アイコン219が表示される。

【0063】「特権」アイコン219の選択により図13に示すようにユーザに対して認められた特権が表示される。この「特権」は「管理」、「サービス」および「フューチャアクセス」が含まれる。

【0064】セキュリティ管理者は通常「セキュリティ」に対する「管理」特権を有し、一方、サイト管理者は「サイト」に対する特権を有している。単独人が「両者」の特権を有することもできる。特定ID番号はユーザには一人の管理者または複数の管理者によって実行される機密保護およびアドミニストレーション機能へのアクセスを得ることができなくなっている。

【0065】図11、図14および図15を参照して、ウインドウ212の「削除」を作動させ、「はい」および「いいえ」のオプションを併せた「ユーザ削除？」を表示する。「はい」の作動で現在のユーザが除かれ、「新規所有者指定」ウインドウ223が表示される。このウインドウを通してセキュリティ管理者が所望ならば現在のシステム中にある前ユーザのジョブを新しい所有者に指定できる。この目的で、図16-17を参照して、「プロフィールオプション」ウインドウ225がオープンされ、「新規ユーザテンプレート」セクション226が表示される。「新規ユーザテンプレート」セクション226の作動により、新しいユーザを作るためにユーザプロフィール215に図17に示されたテンプレート228が表示される。

【0066】同様の工程が続けられ、ここで「新規ユーザ」がユーザに加えられ印刷システム2へのアクセスが可能になる。この場合、「ユーザ名」ファイル205（図10）中の「新規ユーザ」アイコン230が作動される。

【0067】セキュリティ管理者は、あるユーザの独立した機能を設定する能力をも与えられている。この機能はロックアウト前にユーザがサイトのセキュリティレベルに依存して最小ユーザID長さ、最小パスワード長さ等をログオンできるようにすることである。この点において、図10および図18を参照して、セキュリティプロフィールアイコン202が、サイトの現セキュリティ設定を示す「セキュリティプロフィール」スコアカード232を表示するように作動される。この操作にはユーザのログオンが必要であるか否か（「ログオン要」）、ユーザID中の最少キャラクタ数（「最少ユーザID長さ」）、期間の長さ（「期間タイムアウト」）、ユーザによって試みられる許容された最大のログオン長さ（「最大失敗ログオン」）、パスワードの要否（「パスワード要」）、「最小パスワード長さ」、「パスワード経歴長さ」および「パスワード有効期限」が含まれている。

【0068】機密保護に適した機能であるか検査するとき、かつ、システムデータ、ユーザログオン/オフ、保証項目へのアクセス、パワオン/オフ等をモニタし、ログする検査機能を作動させるときに、「アクティビティログ」アイコン235はセキュリティ管理者がデータにアクセスできるようにする。アイコン235の作動により、「ログオン/オフ」等のようなある種の動作のなされた回数をモニタする一連のシステム検査オプションのある「アクティビティログ」スコアカード237(図19)が表示される。「セキュリティコンフィギュレーション」等のサイト機密保護の可能性もセクションのためにオプションと共に表示されアクティビティログ(「プリントアクティビティログ」)のホードコピーをプリントアウトし、また図20に示すようにログ(再初期化アクティビティログ)がリセットされる。

【0069】図10および図21-26を参照して、セキュリティ管理者は共通ファイルへのアクセスを保証しているユーザをまとめているアクセスリストも設定する。「アクセスリスト」アイコン203の作動により選択ウインドウ240を備えた特定ジョブのためにネームのカードファイル239が表示される。前述した各ユーザの場合におけるように、セキュリティ管理者は削除のためのリスト(図23)を選択し、またはリストをオープンしてメンバー名(図24)を表示し、あるいはリストに新規メンバー(図26)を加えることもできる。

【0070】理解できるように、ユーザが特定ジョブまたは個別のジョブで実行を許容されている操作とプログラム選択の組合せはユーザのクイヤランスの直接的結果である。印刷システム2に記憶されたジョブおよびデータへのアクセスに対する制御はデータ製作者または所有者によって作られ、ユーザがシステムに内在しているファイルで実行を許容された操作を制御する。

【0071】図12および図27を参照して、「ジョブアクセス制御」アイコン217の実行により「ジョブアクセス制御」スコアカード241が表示され、印刷システム2に内在するユーザファイルまたはジョブ上でユーザに対して機密保護限定を課することが許容される。機密保護限定は「コピーおよび修正」および「コピー」のみの二つの大きいクラスに分類される。各クラスは「全ユーザ」242、「ジョブ所有者」244、「アクセスリスト」246および「ナン」248に細分類される。「全ユーザ」は全員に対してユーザジョブを変更および(または)コピーが許容される。「ジョブ所有者」はジョブ所有者のみにユーザジョブを変更および(または)コピーの許容されているユーザの名前をリストし、「なし」はユーザジョブの変更および(または)コピーすることをジョブ所有者を含めた全員に対して許容されない。

【0072】修理要員は印刷システム2が製造されたとき、または印刷システム2が据え付けられたときに指定さ

れた修理要員ID番号の形で彼ら自身の機密保護を有する。修理要員ID番号は所望のワークサポートグループレベルまたはあらゆる他のサービスコントロールレベルを制御するのに用いることができる。

【0073】一度、修理要員ID番号が指定されると、修理要員が所属しているサービス機関がパスワードを指定してサービス機関と、正確なパスワードを有する修理要員のみにアクセスを制限するサイトとの両者を保護するように指定される。修理要員パスワードはサービス機関によって随時変更できる。さらに、サービス機関は特定の修理要員パスワードを各サイトに指定して、さらにサイトおよび(または)サービス機関の機密保護必要条件を高めることができる。

【0074】加うるに、サービス機関は各サイトにおける選ばれた個人に対する高レベルのアクセスサービスを指定することもできる。典型的に、このサービスは典型的なユーザが行なうことのできるより困難で複雑なサービス操作を印刷システム2に対して実行できる指定のトレーニングコースに参加したサイト担当者に対するものである。サイト管理者はこの目的でセキュリティ管理者に対して、通常図13に示すように「特権」下の「サービス」の選択によって特定サービスアクセス権を調整させるために選ばれるべきサイト担当者を決定する。

【0075】ファイルがパスワード機構および(または)ユーザの能力によって保護され、前述したようにユーザのファイルに対して他人の適当なアクセス権が決定されるが、オペレータもセキュリティラベルをファイルに指定する能力を有するセキュリティラベルの使用を可能にするために、ヘンスト(Hengst)らの名義で「電子印刷機で作成された印刷物をもつマージログのための方法」の名称で1990年9月28日に出願された米国特許出願第590633号(代理人整理番号D/89288)に開示されているシステムがこの目的に使用可能である。セキュリティラベルのホルダはオペレータが自分のセキュリティラベルを置くシステムマージライブラリに記憶される。この記憶をすることにおいて、ユーザはセキュリティラベルが現われているページおよびページサイド上のセキュリティラベルの位置を認識することができる。印刷システム2は一度選ばれることが保証されると、ユーザファイルが現在のユーザによって選択されたセキュリティラベルなしにはタッチスクリーン62に指示されたり、プリンタ部8によって印刷されることは決してない。加うるに、印刷システム2はオペレータに対してタッチスクリーン62上に表示された、またはプリンタ部8によって印刷されたイメージのバックグラウンドにセキュリティラベルを置くオプションを与える。こうすることによって、セキュリティラベルがイメージそのものと直接関係して現われるので、だれでもラベルが除去されるのを回避できる。

【0076】セキュリティラベルに加えて、印刷システ

ム2は表示された、または印刷されたイメージの一つのエッジまたは両エッジに沿って自動日時スタンプを有するラベル、プリントをする印刷システムのサイトを識別するラベル、イメージ所有者を識別するラベル等々のような他のラベルの印刷能力を備えている。

【0077】図28を参照して、印刷システム2の内部のセキュリティシステムにつき示し、説明したが、一つまたはそれ以上のサイトのセキュリティの制御もここではセキュリティセンター300として示した遠隔サイトから確立される。セキュリティセンター300は電話線10のような通信チャネル305によって一つの印刷システムサイトまたは複数サイトに接続されている。セキュリティセンター300における外部データベースまたはデータベースが、ユーザの「ユーザプロフィール」215およびセキュリティ管理者による確立に基づくID番号としての記憶媒体の働きをする。ユーザの個々のパスワードはユーザによって用いられる印刷システムの内部データベースまたはメモリ56に記憶される。

【0078】一つまたはそれ以上の印刷システム2へのアクセスを得るためにユーザはキーボード64を用いて20ユーザID番号およびパスワードを登録する。ユーザID番号はチャネル305を介して外部データベース308で保持され、ユーザID番号により実行される。ユーザによってサイトに登録されたユーザID番号がデータベース308に保持された番号と一致する場合には、証明信号がチャネル305を介して印刷システムのコントローラ部7に送られて、ユーザが証明される。同時にユーザによって登録されたパスワードがシステム内部データベースに保持されたパスワードと比較され、一致がある場合には、第2証明信号が発生され、印刷システムの40コントローラ部7に送られる。ユーザの証明が受信されると、コントローラ部7がユーザの印刷システムへのアクセスを可能にする。

【図面の簡単な説明】

【図1】 本発明の機密保護システムに併用する電子印刷システムを示す図である。

【図2】 図1に示す印刷システムの主要素を示すブロック図である。

【図3】 図1に示す印刷システムの主たる機械要素を示す平面図である。

【図4】 図1に示す印刷システムの文書スキャナの特定制部分の構造の詳細を示す説明図である。

【図5】 図1に示す印刷システムのコントローラ部の主要部を示すブロック図の1である。

【図6】 図1に示す印刷システムのコントローラ部の主要部を示すブロック図の2（続き）である。

【図7】 図1に示す印刷システムのコントローラ部の主要部を示すブロック図の3（続き）である。

【図8】 図1に示す印刷システムのための操作システムをプリント配線基板および共通ライン接続と共に示す50

ブロック図である。

【図9】 図1に示す印刷システムのユーザインタフェース（UI）タッチスクリーン上に表示された典型的なジョブプログラミングチケットおよびジョブスコアカードを示す図である。

【図10】 ユーザインタフェースタッチスクリーンを示す図である。

【図11】 ユーザがハイライトすることと、プロセスセクションを規定するシステム管理者ウインドウをオープンすることによって選択されることを示す図である。

【図12】 選択されたユーザのユーザプロフィールを表示する図である。

【図13】 選択されたユーザの「特権」カードファイルを示す図である。

【図14】 オープンされた「ユーザ削除？」オプションウインドウを示す図である。

【図15】 オープンされた「新規所有者選定？」オプションウインドウを示す図である。

【図16】 オープンされた「ユーザプロフィールオプション」ウインドウを示し、「新規ユーザテンプレート」セクションを表示する図である。

【図17】 「新規ユーザテンプレート」次選択を示すユーザインタフェースタッチスクリーンを示す図である。

【図18】 サイト用「セキュリティプロフィール」カードファイルを示す図である。

【図19】 サイト用「アクティビティログ」を示す図である。

【図20】 図19の「アクティビティログ」をオープンされた「オーディットトレイルオプション」ウインドウと共に示す図である。

【図21】 「アクセスリスト」カードファイルを表わすユーザインタフェースタッチスクリーンを示す図である。

【図22】 リストセクションを表示すべくオープンされたファイルウインドウと共に図21の「アクセスリスト」カードファイルを示す図である。

【図23】 オープンされた「リスト削除？」ウインドウと共に図21の「アクセスリスト」カードファイルを示す図である。

【図24】 選択されたアクセスリスト中のメンバーの名前で「メンバー名」ファイルを示す図である。

【図25】 選択されたアクセスリストからメンバーを除外する「リストからの消去」選択ウインドウを示す図である。

【図26】 選択されたアクセスリストにメンバーの名前を加えるための「メンバー追加」ウインドウを示す図である。

【図27】 ファイル所有者をしてアクセス権をファイ

17

ル所有者に設定せしめる「ジョブアクセス制御」カードを示す図である。

【図28】 機密保護システムが外部から管理される第2実施例を示す図である。

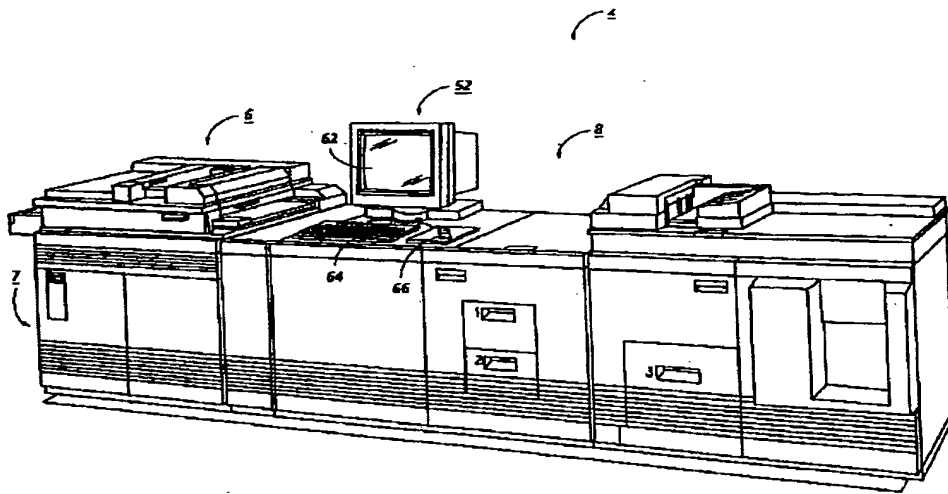
【符号の説明】

2 イメージ印刷システム、4 イメージ入力セクション、5 ネットワーク、7 コントローラセクション、

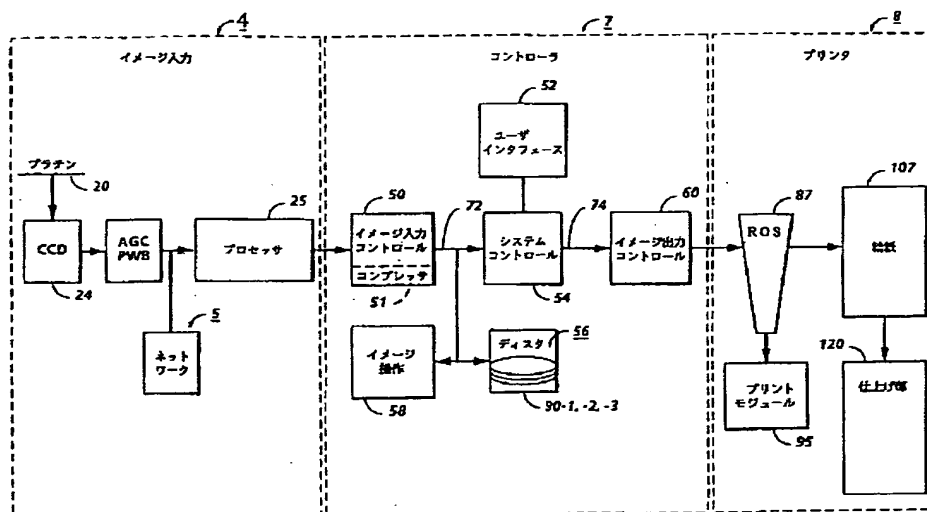
18

8 プリンタセクション、20 プラテン、24 CCDカメラ、25 プロセッサ、50 イメージ入力コントロール、51 イメージ圧縮装置、52 ユーザインタフェース、54 システムコントローラ、58 イメージ操作装置、56 ディスク、60 イメージ出力コントロール、87 ラスタ出力スキャナ、95 印刷モジュール部、107 給紙部、120 仕上げ機

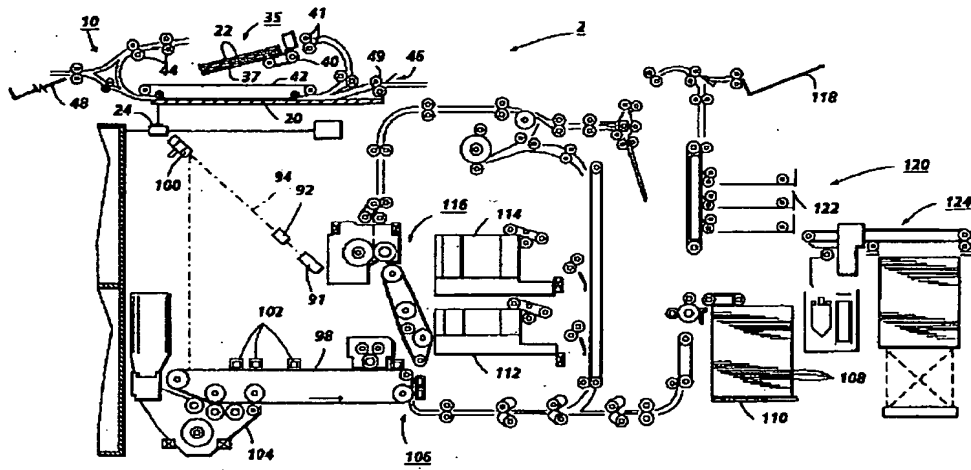
【図1】



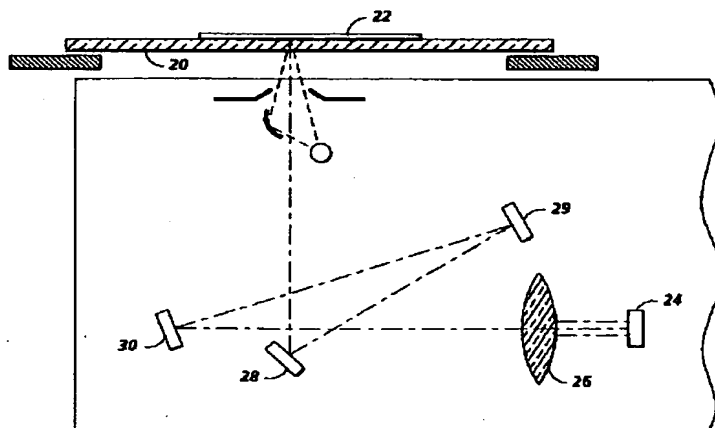
【図2】



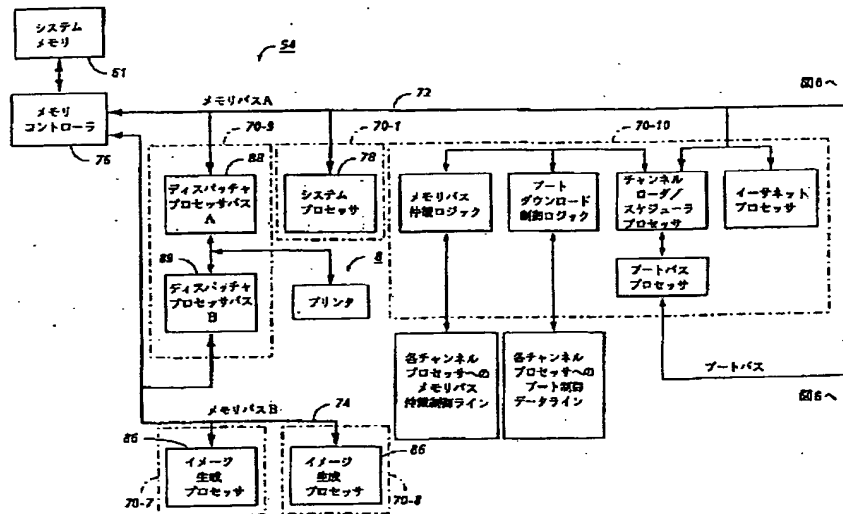
【図3】



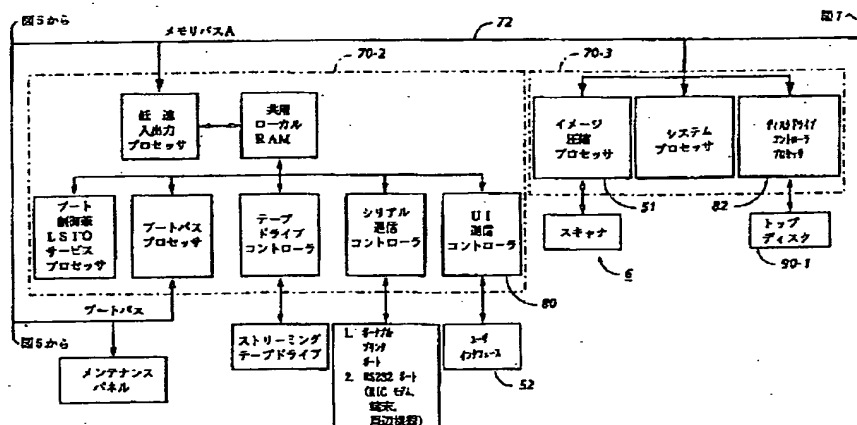
【図4】



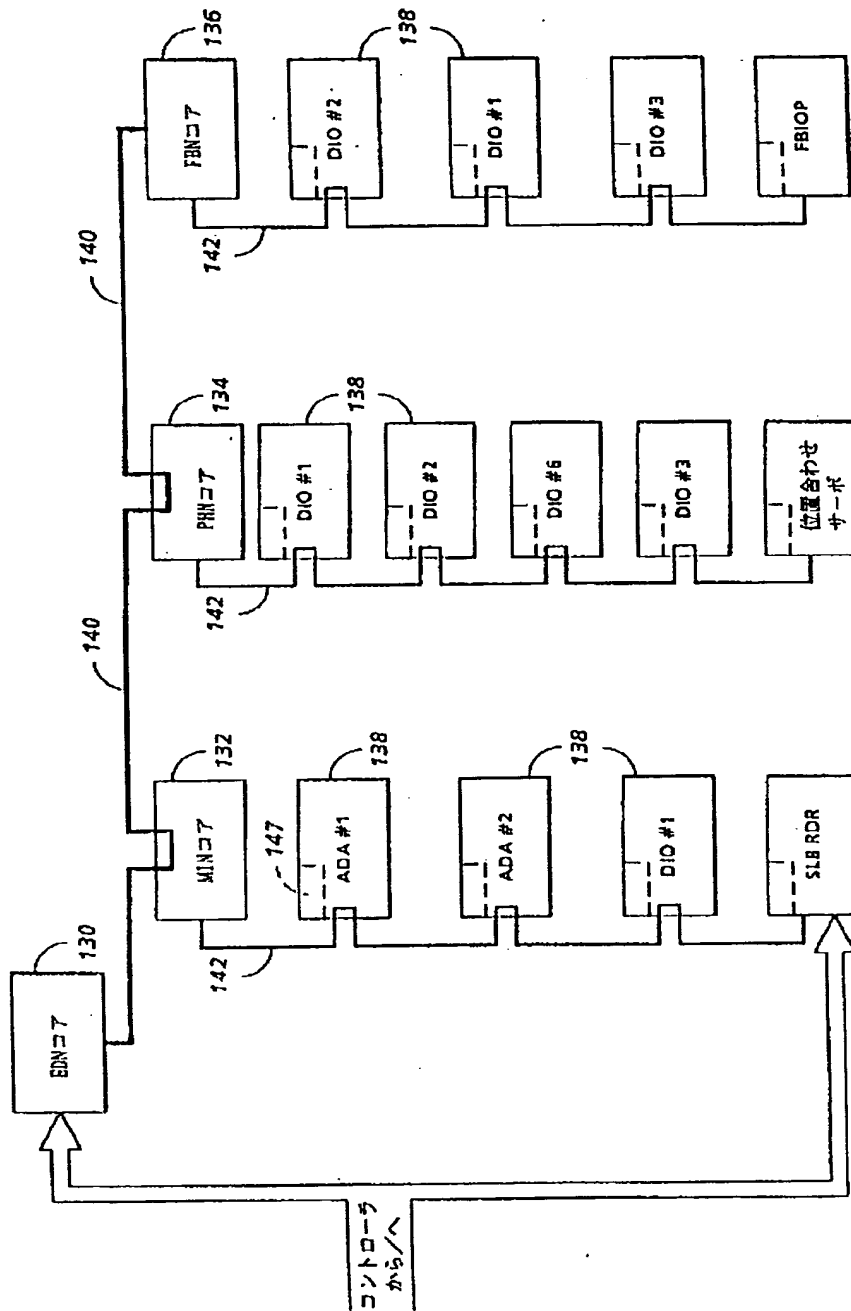
【図5】



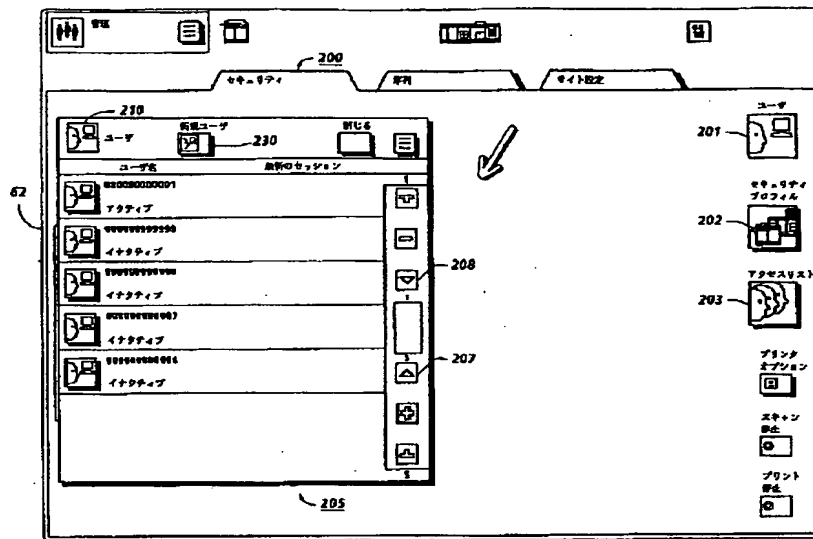
【図6】



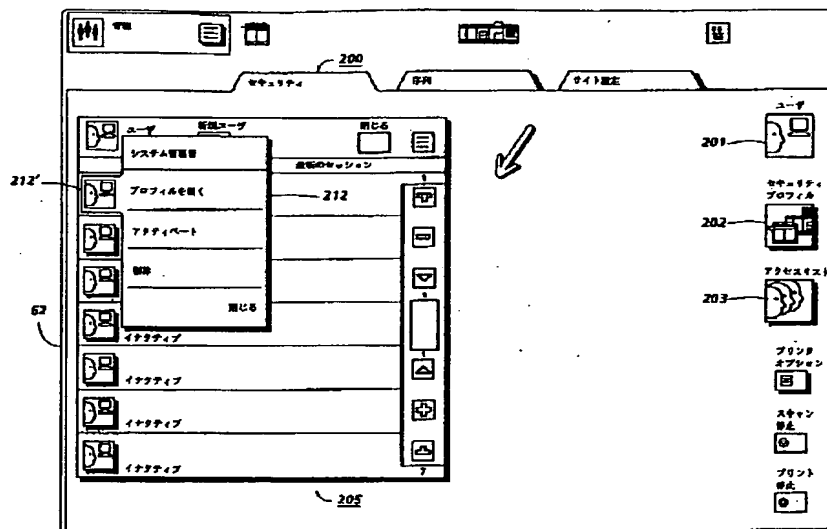
【図8】



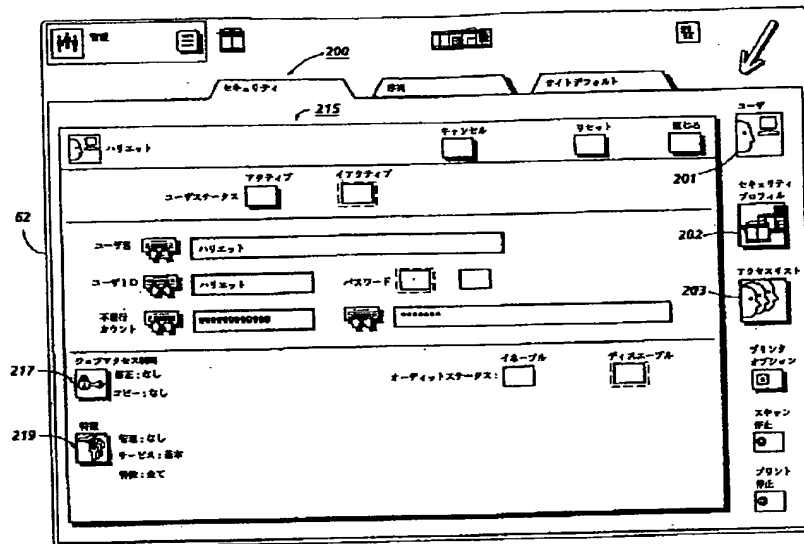
【図10】



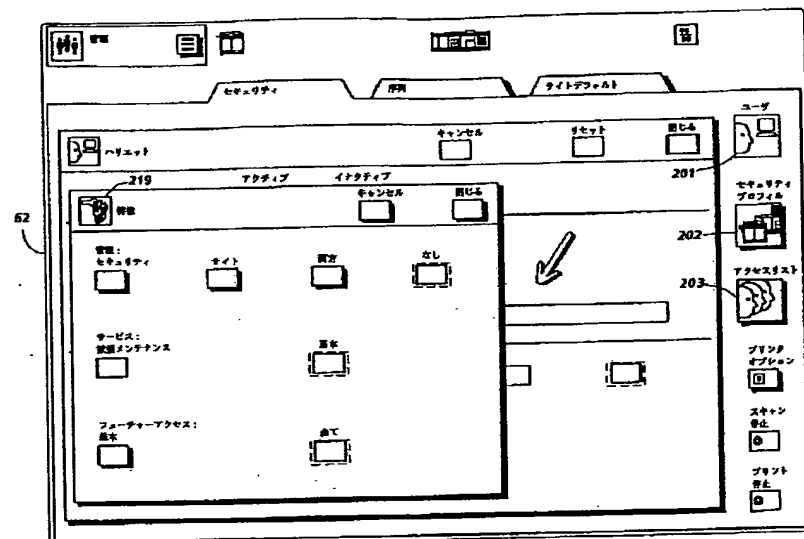
【図11】



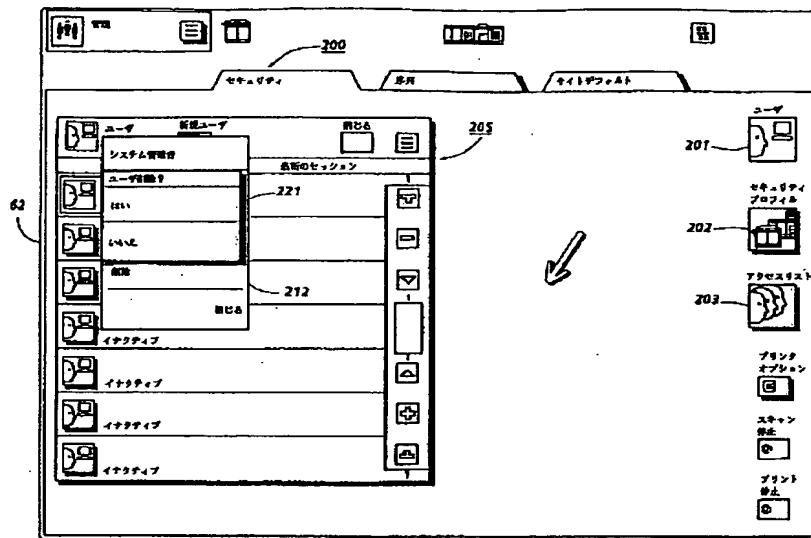
【図12】



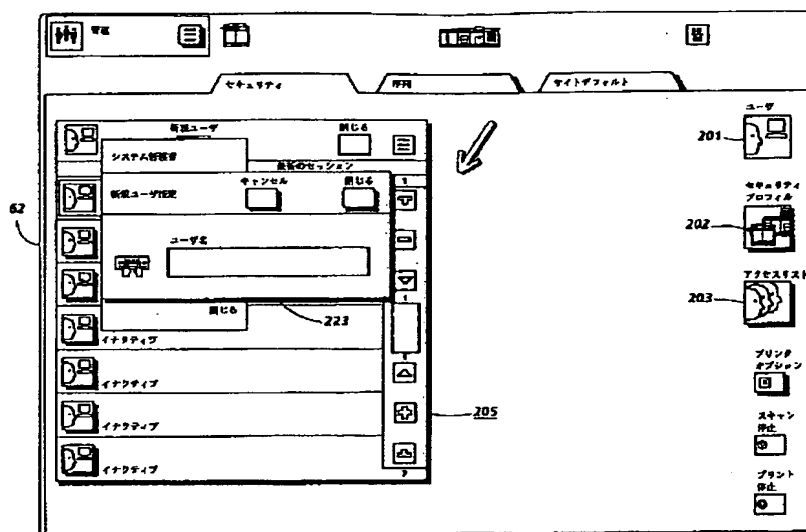
【図13】



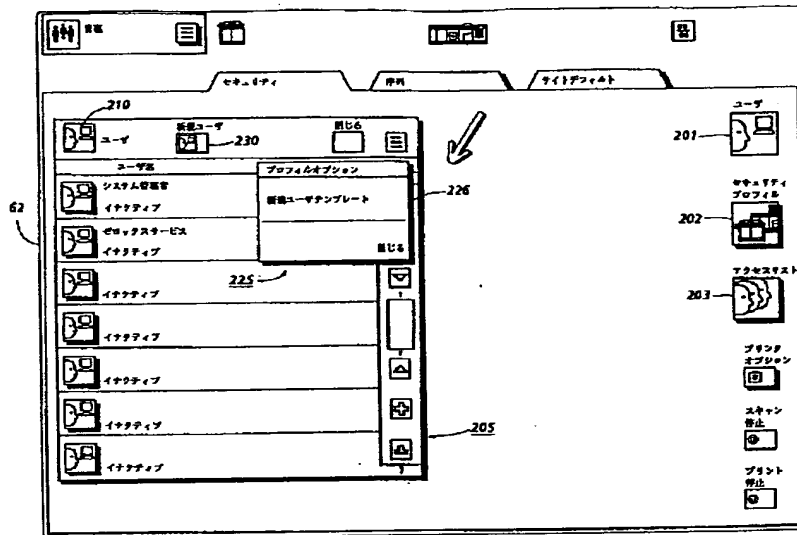
【図14】



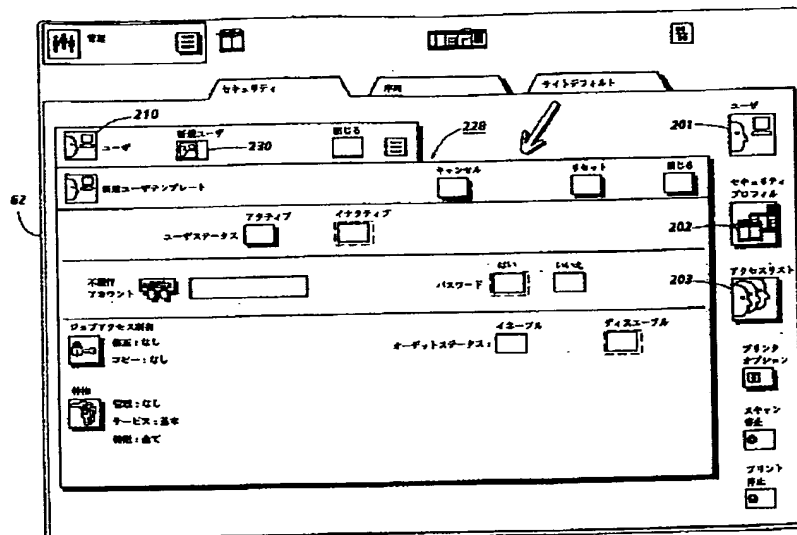
【図15】



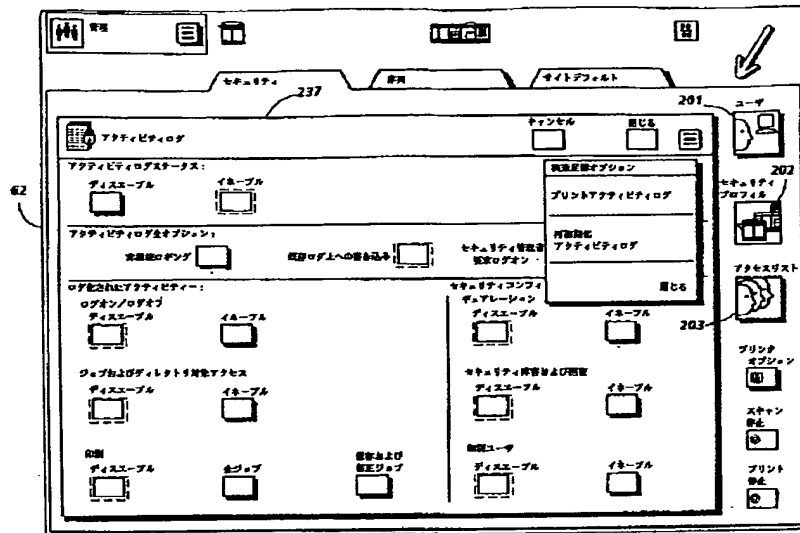
【図16】



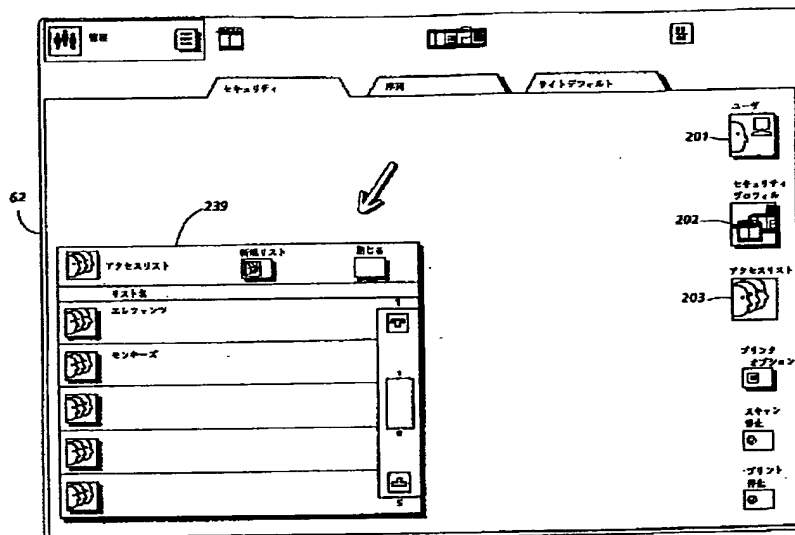
【図17】



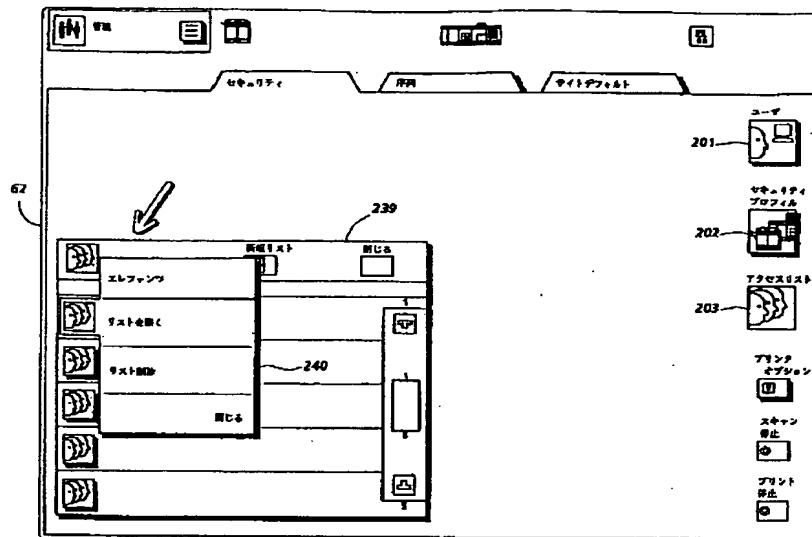
【図20】



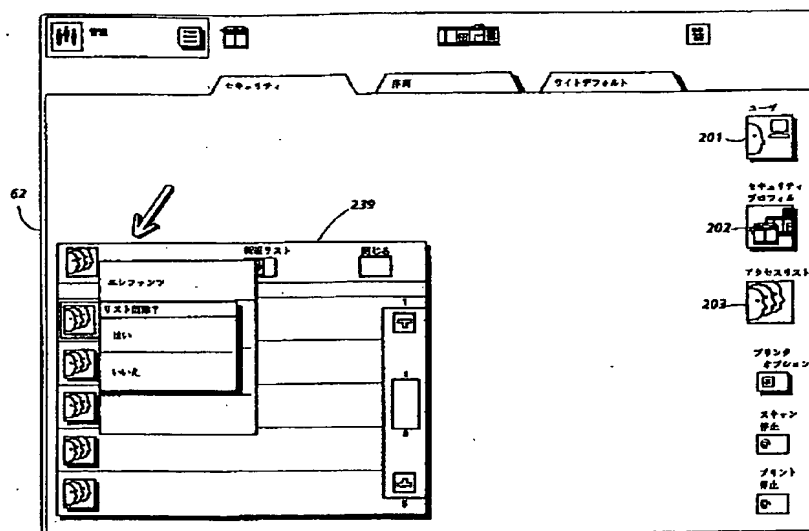
【図21】



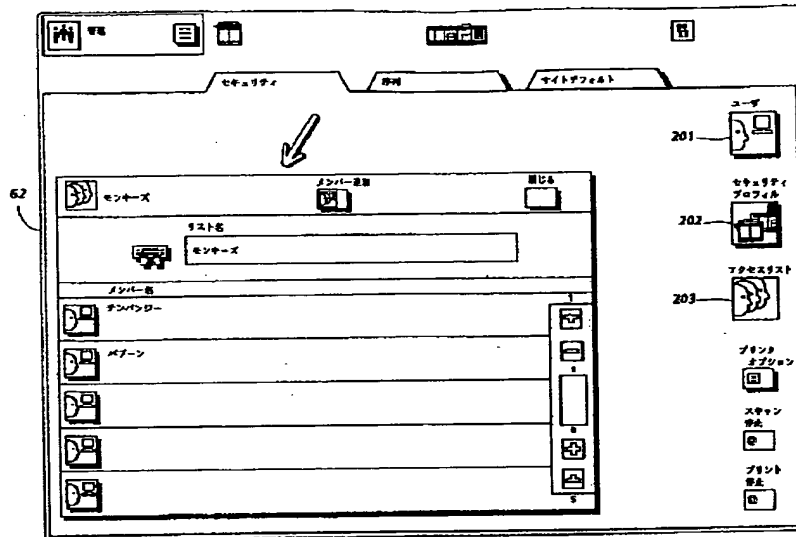
【図22】



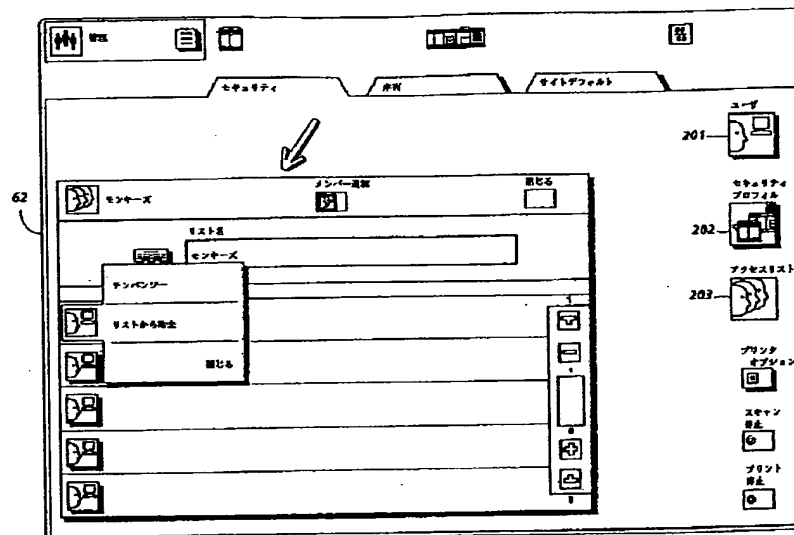
【図23】



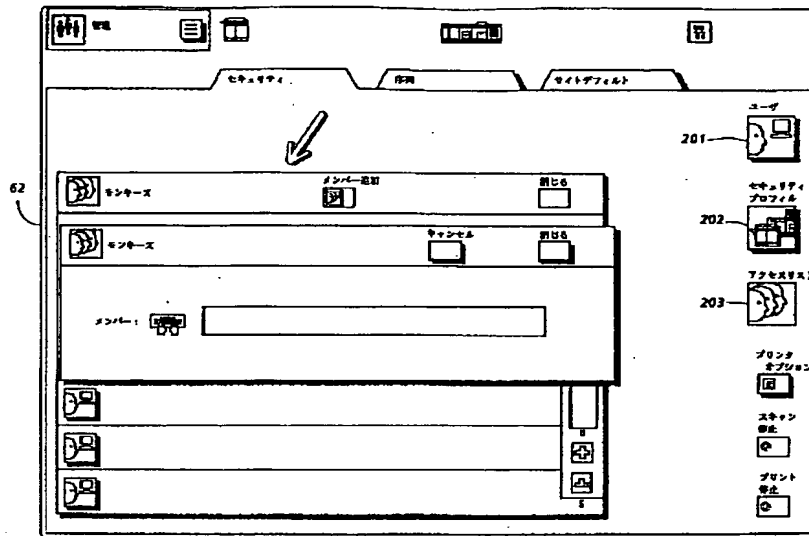
【図24】



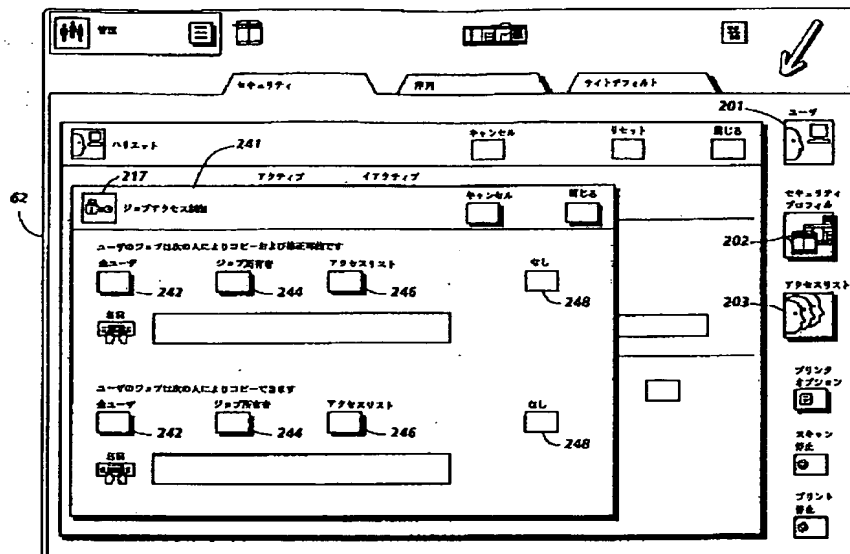
【図25】



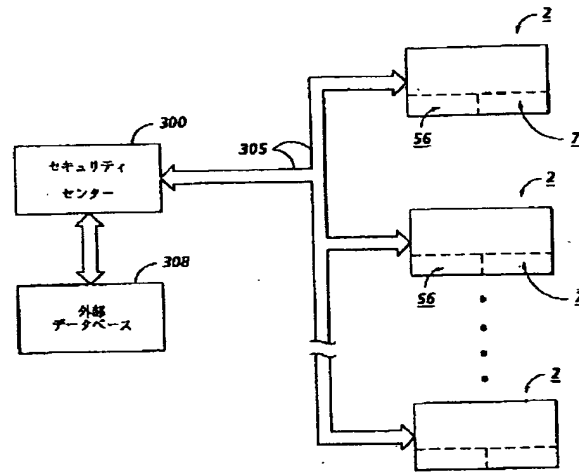
【図26】



【図27】



【図28】



フロントページの続き

(72)発明者 ピーター・デュー・ウイング
 アメリカ合衆国 ニューヨーク州 14580
 ウェブスター ヘフナードライブ 94

(72)発明者 ジャック・エフ・ラットクリフ・ザ・セカ
 ンド
 アメリカ合衆国 ニューヨーク州 14534
 ビッツフォード サンセットブルバ
 ード 19

(72)発明者 ポール・ジェイ・バリエール
 アメリカ合衆国 ニューヨーク州 14450
 フェアポート グリムスピーゲート 15